REMARKS/ARGUMENTS

This paper is being provided in response to the August 24, 2005 Office Action for the above-referenced application. In this response, Applicant has amended Claims 1, 12, 16, 25, 29, 59, 74, 83, and 87 in order to clarify that which Applicant deems to be the claimed invention. Applicant respectfully submits that the amendments to the claims are all supported by the originally filed application.

In response to the rejection of Claims 1-31, and 59-89 under 35 U.S.C. 101, Applicant has amended independent Claims 1 and 59 in accordance with remarks set forth in the Office Action. Applicant's amended Claim 1 recites a computer-implemented method for generating a pruned augmented attack tree. Applicant respectfully submits that the pruned augmented attack tree is formed as a result of the claimed method. The method recites steps for building the tree including adding nodes and edges to the tree. Accordingly, Applicant respectfully submits that Claims 1 and 31, and all claims depending therefrom, are now directed to statutory subject matter under 35 U.S.C. 101. In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 1-3, 7-10, 16-19, 25-30, 59-61, 65-68, 74-77 and 83-88 under 35 U.S.C. § 103(a) as being unpatentable over Adler, U.S. 20030149777 (hereinafter referred to as "Adler") in view of Cline et al., U.S. Patent No. 5,313,616 (hereinafter referred to as "Cline") is hereby traversed and reconsideration thereof is respectfully requested. Applicant respectfully submits that Claims 1-3, 7-10, 16-19, 25-30, 59-61, 65-68, 74-77 and 83-88, as amended herein, are patentable over the cited references.

Claim 1, as amended herein, recites a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree. Claims 2-3, 7-10, 16-19, and 25-30 depend from Claim 1.

Claim 59, as amended herein, recites a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said

inserts in accordance with said determines, said pruned augmented attack tree being a pruned version of a full attack tree. Claims 60-61, 65-68, 74-77 and 83-88 depend from Claim 59.

Adler relates to probabilistic packet marking in network systems. (Par. 2). Adler's Figure 2 includes a network of nodes 24 and a victim 26. The network of nodes represents, for example, routers. On the Internet, a router is a device that determines the next network point to which a packet should be forwarded toward its destination. From a perspective of the victim 26, a routing topology of the network 24 is an inverted binary tree. Any packet sent to the victim from the attacker 22 travels down the tree until the packet reaches victim 26. At the start of the attack, attacker 22 chooses the network of nodes 24 of the tree, and then for each packet, it determines which of these nodes 24 sends that packet to the victim 26. (Par. 21).

Cline is cited on page 4 of the Office Action as support for pruning a tree (Col. 13, Lines 31-43). Cline discloses removing a dead branch from a tree corresponding to code that will never be executed. Removal of such a branch produces a "pruned" tree.

Applicant's Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest the features of ***a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already***

included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree, as set forth in Claim 1. Adler and Cline neither disclose nor suggest an attack tree or generating an attack tree. Rather, Adler's tree represents network topology in terms of routers traversed on a path from the perspective of the victim, and Cline's tree appears to be a graph of basic blocks of instructions of an application program. Adler, in fact, does not appear to describe how to generate the tree used therein, but rather appears to set forth what the tree represents (e.g., router topology).

As discussed above, page 4 of the Office Action cites Cline, Col. 13, lines 13-43, as teaching pruning a tree. Cline neither discloses nor suggests pruning an attack tree. Rather, Cline discloses removing branches of a tree corresponding to dead code. Cline discloses pruning a path of the tree by determining whether the associated code is never executed. Cline neither discloses nor suggests the condition set forth in Applicant's amended Claim 1 of ***determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node***, as set forth in amended Claim 1.

Additionally, Applicant respectfully submits that Adler's technique cannot possibly accommodate any type of pruning between the attacker's router and the victim's router, since applying such pruning would make the router trace data inaccurate. The entire path between attacker and victim must be represented in Adler. Accordingly, Adler appears to teach away from any use of pruning. Furthermore, based on the foregoing, Applicant respectfully submits that one of ordinary skill in the art would not be motivated to combine Adler with any pruning technique disclosed in any reference.

For at least these reasons, Applicant respectfully submits that the references neither teach, disclose, nor suggest at least the foregoing recited features of Applicant's amended Claim 1.

For reasons similar to those set forth regarding Claim 1, Applicant's Claim 59, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest the features of ***a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said inserts in accordance with said determines,***

said pruned augmented attack tree being a pruned version of a full attack tree, as set forth in Claim 59.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 4-6, 20-24, 31, 62-64, 78-82 and 89 under 35 U.S.C. § 103(a) as being unpatentable over Adler and Cline and further in view of Schneier, U.S. Patent No. 5,850,516 (hereinafter referred to as "Schneier") is hereby traversed and reconsideration thereof is respectfully requested. Applicant respectfully submits that 4-6, 20-24, 31, 62-64, 78-82 and 89 are patentable over the cited references.

Claims 4-6, 20-24, and 31 depend from independent Claim 1. Claims 62-64, 78-82 and 89 depend from independent Claim 59. For reasons set forth above, Claims 1 and 59, and claims that depend therefrom, are neither disclosed nor suggested by Adler and Cline. For reasons set forth below, Applicant respectfully submits that combining Adler and Cline with Schneier also neither disclose nor suggest Claims 1 and 59, or claims that depend therefrom.

Schneier is cited in the Office Action at page 8 as support for disclosing an edge from a first node at level x to a second node at level x+1 representing an action while in a first state including a first attacker state corresponding to said first node resulting in a second state including a second attacker state. (Col. 6, Lines 25-47). Schneier discloses an attack tree is a tree structure where the root node is the goal of the attacker, leaf nodes are the attacker's possible

actions, and the intermediate nodes represent various combinations of the attacker's actions that may achieve this goal. (Col. 6, Lines 44-47).

Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest the features of ***a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 1. For reasons set forth above, Adler and Cline neither disclose nor suggest the foregoing recited features of Claim 1. Schneier appears silent regarding how to generate the attack trees used therein. Schneier discloses an attack tree where the root node is the goal of the attacker, not a root node which is a starting point of an attack. Accordingly, Schneier also appears silent regarding any disclosure or suggestion of the foregoing features of Claim 1. Thus, combining Adler and Cline with Schneier does not overcome the deficiencies of Adler and Cline with respect to the foregoing features of Claim 1.

Applicant further submits that one of ordinary skill in the art would not be motivated to combine any technique used in connection with Schneier's attack tree with trees used in Adler or Cline since the trees used in Adler or Cline are not attack trees. Rather, as described above, Adler's tree represents network topology in terms of routers traversed on a path from the perspective of the victim, and Cline's tree appears to be a graph of basic blocks of instructions of an application program.

For at least these reasons, Applicant respectfully submits that the references neither teach, disclose, nor suggest at least the foregoing recited features of Applicant's amended Claim 1.

For reasons similar to those set forth regarding Claim 1, Claim 59 is also neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest of ***a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said inserts in accordance with said determines, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 59.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 13 and 71 under 35 U.S.C. § 103(a) as being unpatentable over Adler and Cline and further in view of Swiler et al, (Computer Attack Graph Generation Tool, hereinafter referred to as "Swiler") is hereby traversed and reconsideration thereof is respectfully requested. Applicant respectfully submits that Claims 13 and 71 are patentable over the cited references.

Claim 13 depends from Claim 1. Claim 71 depends from Claim 59. For reasons set forth above, Claims 1 and 59, and claims that depend therefrom, are neither disclosed nor suggested by Adler and Cline. For reasons set forth below, Applicant respectfully submits that combining Adler and Cline with Swiler also neither discloses nor suggests Claims 1 and 59, and claims that depend therefrom.

Swiler is cited on page 9 of the Office Action as support for disclosing that the pruned augmented attack tree has a property that a resulting node at a level "n+1" and an edge connecting a current node at level "n" to the resulting node are included in the pruned augmented attack tree if the edge and the resulting node are not already included in the pruned augmented attack tree with the edge connecting an ancestor of the current node to an instance of the resulting node, the ancestor being a node at level "x" < "n" and the instance of the resulting node being at level "x+1". (See section 3.3).

Applicant's Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest the features of ***a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 1. For reasons set forth above, Adler and Cline neither disclose nor suggest the foregoing recited features of Claim 1. Swiler appears silent regarding any disclosure or suggestion of the forgoing recited features. Thus, combining Adler and Cline with Swiler does not overcome the deficiencies of Adler and Cline with respect to the foregoing features of Claim 1.

For reasons similar to those set forth regarding Claim 1, Claim 59 is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest of ***a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with***

respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said inserts in accordance with said determines, said pruned augmented attack tree being a pruned version of a full attack tree, as set forth in Claim 59.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 14 and 72 under 35 U.S.C. § 103(a) as being unpatentable over Adler and Cline and further in view of Ammann et al, (Scalable, Graph-Based Network Vulnerability Analysis, hereinafter referred to as "Ammann") is hereby traversed and reconsideration thereof is respectfully requested. Applicant respectfully submits that Claims 14 and 72 are patentable over the cited references.

Claim 14 depends from Claim 1. Claim 72 depends from Claim 59. For reasons set forth above, Claims 1 and 59, and claims that depend therefrom, are neither disclosed nor suggested by Adler and Cline. For reasons set forth below, Applicant respectfully submits that combining

Adler and Cline with Ammann also neither discloses nor suggests Claims 1 and 59, and claims that depend therefrom.

Ammann is cited on page 11 of the office action as support for disclosing determining which hosts in said network are equivalent forming a group; and representing said group with a single host. (See page 223, right column).

Applicant's Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest the features of ***a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 1. For reasons set forth above, Adler and Cline neither disclose nor suggest the foregoing recited features of Claim 1. Ammann appears silent regarding any disclosure or suggestion of the forgoing recited

features. Thus, combining Adler and Cline with Ammann does not overcome the deficiencies of Adler and Cline with respect to the foregoing features of Claim 1.

For reasons similar to those set forth regarding Claim 1, Claim 59 is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest ***a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said inserts in accordance with said determines, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 59.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 11-12 and 69-70 under 35 U.S.C. § 103(a) as being unpatentable over Adler, Cline and Schneier and further in view of Swiler is hereby traversed and

reconsideration thereof is respectfully requested. Applicant respectfully submits that Claims 11-12 and 69-70 are patentable over the cited references.

Claims 11-12 depend from Claim 1. Claims 69-70 depend from Claim 59. For reasons set forth above, Claims 1 and 59, and claims that depend therefrom, are neither disclosed nor suggested by Adler, Cline and Schneier. For reasons set forth below, Applicant respectfully submits that combining Adler, Cline and Schneier with Swiler also neither discloses nor suggests Claims 1 and 59, and claims that depend therefrom.

Swiler is cited on page 12 of the Office Action as support for disclosing evaluating each action that exploits a vulnerability of a host in accordance with connectivity data (see section 2.2) wherein said connectivity data, said each action, and said vulnerability are stored in a database and determined prior to performing said generating (see sections 3.1 and 3.2.1).

Applicant's Claim 1, as amended herein, is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest ***a computer-implemented method for generating a pruned augmented attack tree comprising: receiving a starting point of a computer attack with respect to a network; inserting a root node into said pruned augmented attack tree for said starting point; determining whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said augmented pruned attack tree in accordance***

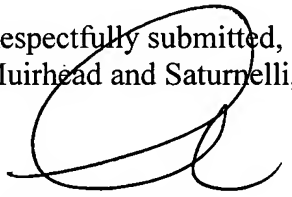
with said determining, said determining being repeatedly performed for nodes inserted into said pruned augmented attack tree, said inserting being repeatedly performed in accordance with said determining, said pruned augmented attack tree being a pruned version of a full attack tree, as set forth in Claim 1. For reasons set forth above, Adler, Cline and Schneier do not disclose or suggest the foregoing recited features of Claim 1. Swiler appears silent regarding the foregoing recited features of Claim 1. Thus, combining Adler, Cline and Schneier with Swiler does not overcome the deficiencies of Adler, Cline and Schneier with respect to the foregoing recited features of Claim 1.

For reasons similar to those set forth regarding Claim 1, Claim 59 is neither disclosed nor suggested by the references, taken separately or in combination, in that the references neither disclose nor suggest ***a computer program product for generating a pruned augmented attack tree comprising executable code that: receives a starting point of a computer attack with respect to a network; inserts a root node into said pruned augmented attack tree for said starting point; determines whether, for a current node included in said pruned augmented attack tree, to add to said pruned augmented attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said pruned augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; inserts nodes and edges into said augmented pruned attack tree in accordance with said determines, repeatedly performing said determines for nodes inserted into said pruned augmented attack tree, repeatedly performing said inserts in accordance with said determines, said pruned augmented attack tree being a pruned version of a full attack tree,*** as set forth in Claim 59.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

Based on the above, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 508-898-8604.

Respectfully submitted,
Muirhead and Saturnelli, LLC



Anne E. Saturnelli
Reg. No. 41,290

Muirhead and Saturnelli, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
Tel: (508) 898-8601
Fax: (508) 898-8602

Date: November 30, 2005